(12) UK Patent Application (19) GB (11) 2 223 614 (13) A

(43) Date of A publication 11.04.1990

(21) Application No 8820470.6

(22) Date of filing 30.08.1988

(71) Applicant
Gerald Victor Waring
26 Lynwood Chase, Bracknell, Berkshire,
United Kingdom

(72) Inventor
Gerald Victor Waring

(74) Agent and/or Address for Service
Withers & Rogers
4 Dyer's Buildings, Holborn, London, EC1N 2JT,
United Kingdom

(51) INT CL⁴
A61B 5/00, G06K 9/00, H04N 1/21

(52) UK CL (Edition J)
G4R RRM R1X R10E R11D R11E R12A R4A2 R5B R8A R9B
H4F FAA FS24 FS25R FS42C FS83C
U1S S1714 S2120 S2142

(56) Documents cited
GB 2173970 A GB 2173933 A GB 2143980 A
GB 1403765 A

(58) Field of search
UK CL (Edition J) G4R REF RET REX RPF RPQ RPX RRH RRL RRM RRP RRQ RRT, H4F
INT CL⁴ A61B, G06K, G07C, H04N

(54) Identity verification

(57) A security device for identifying the user of the device has a non-volatile memory which stores picture data representative of a picture of the user's face. When the device, which may be in the form of a key with electrical contacts, or a card, is presented to a key reading terminal (48), the picture data is read from the memory and decoded to produce a picture on a display (42) which can then be visually compared with the user by security personnel. The comparison can be carried out at a remote station by using a television camera (52) to view the user at the terminal. Compression of the picture data prior to storage in the memory of the security device is performed by grey scale level reduction and pixel averaging to reduce resolution.

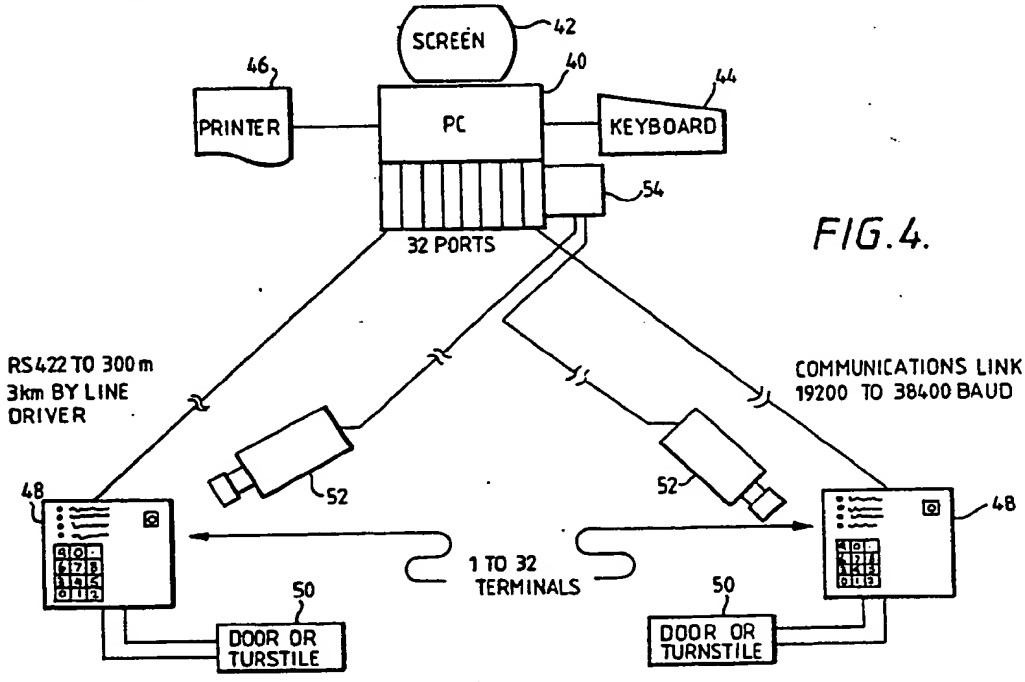


FIG.4.

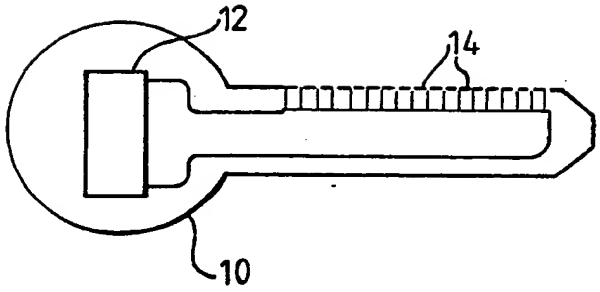

12
14
10

FIG. 1.

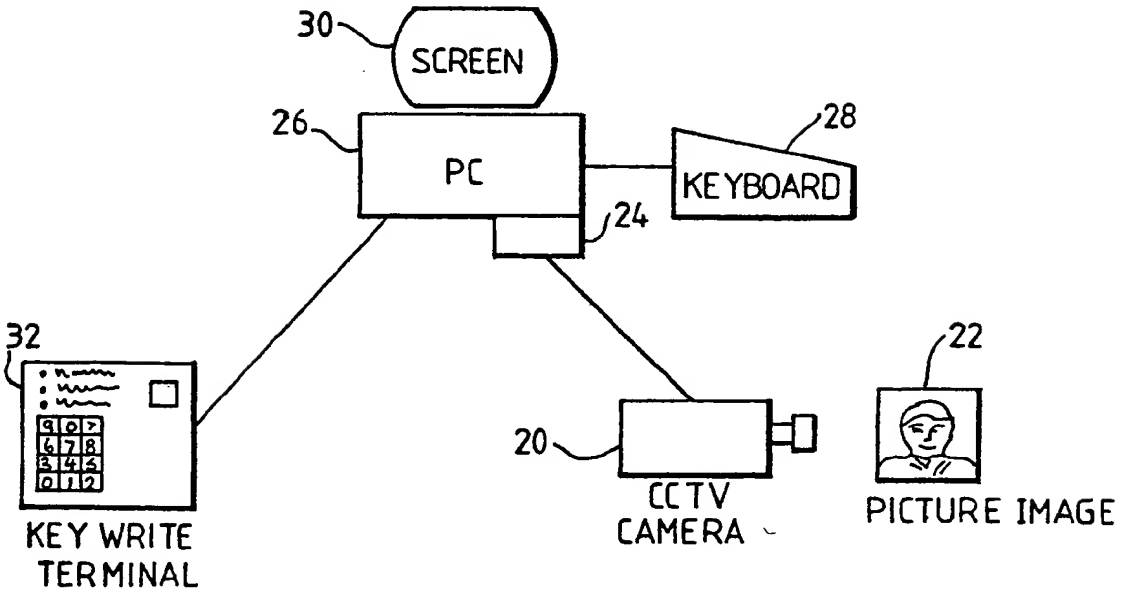

30
SCREEN
26
PC
28
KEYBOARD
24
32
22
20
CCTV
CAMERA
PICTURE IMAGE
KEY WRITE
TERMINAL

FIG. 2.

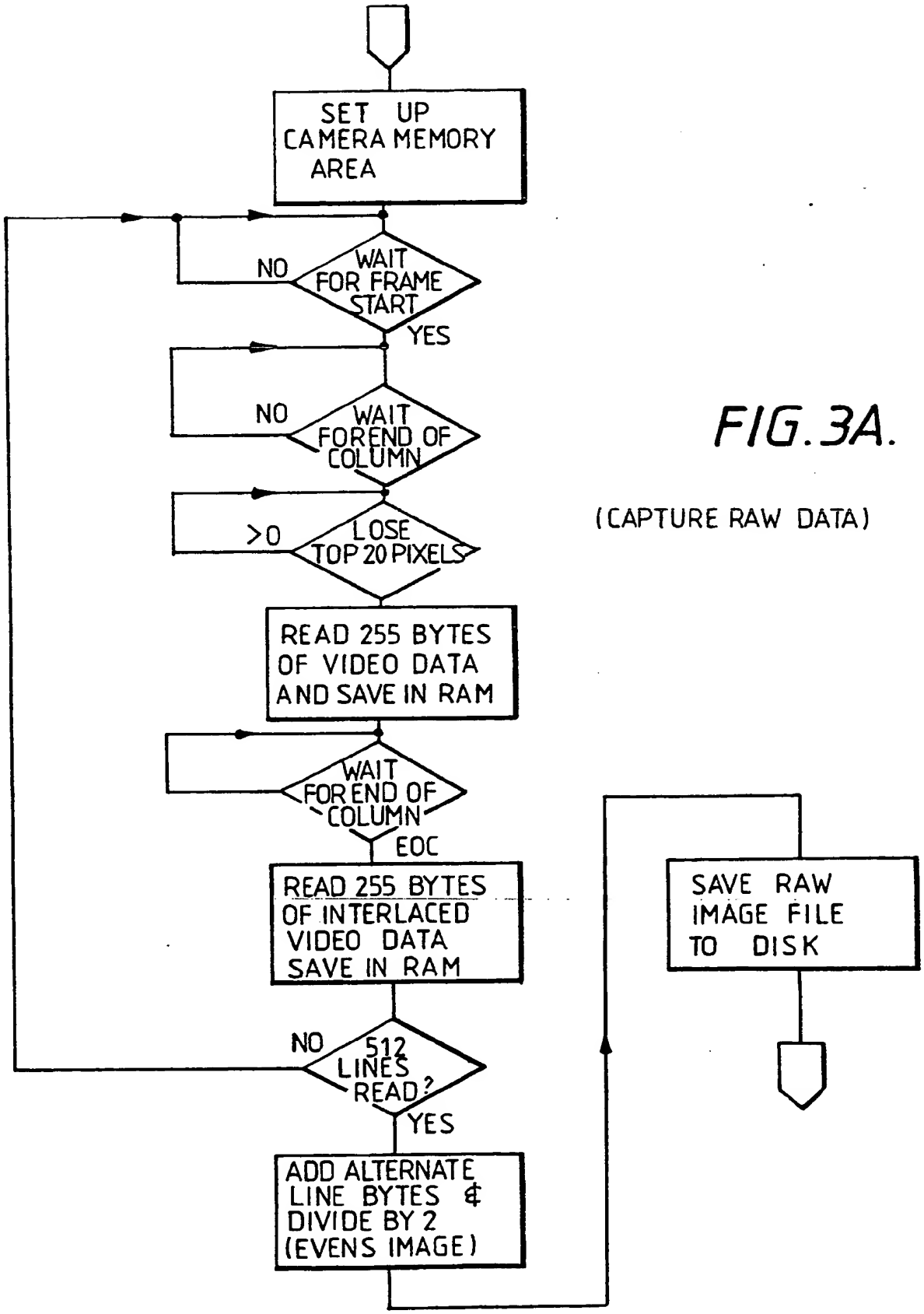


FIG. 3A.

(CAPTURE RAW DATA)

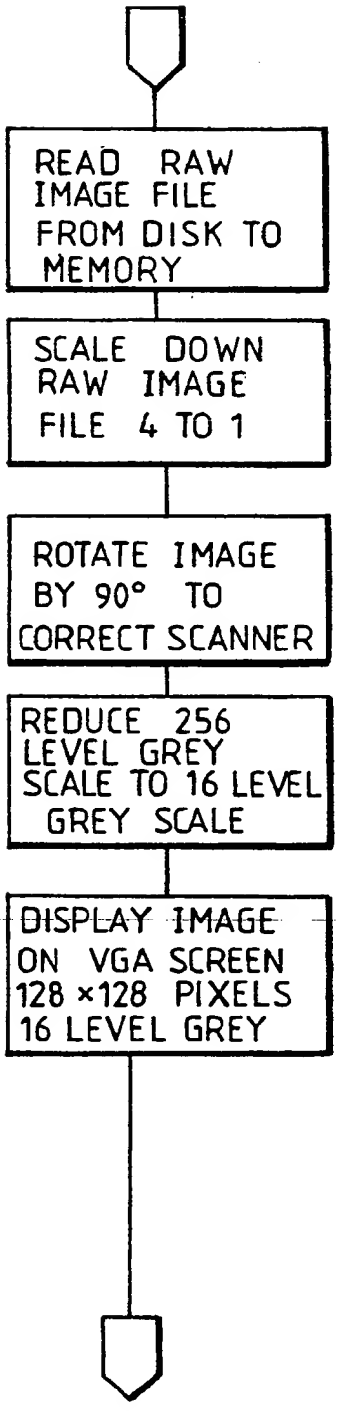


FIG. 3B.

(DISPLAY RAW IMAGE ON SCREEN)

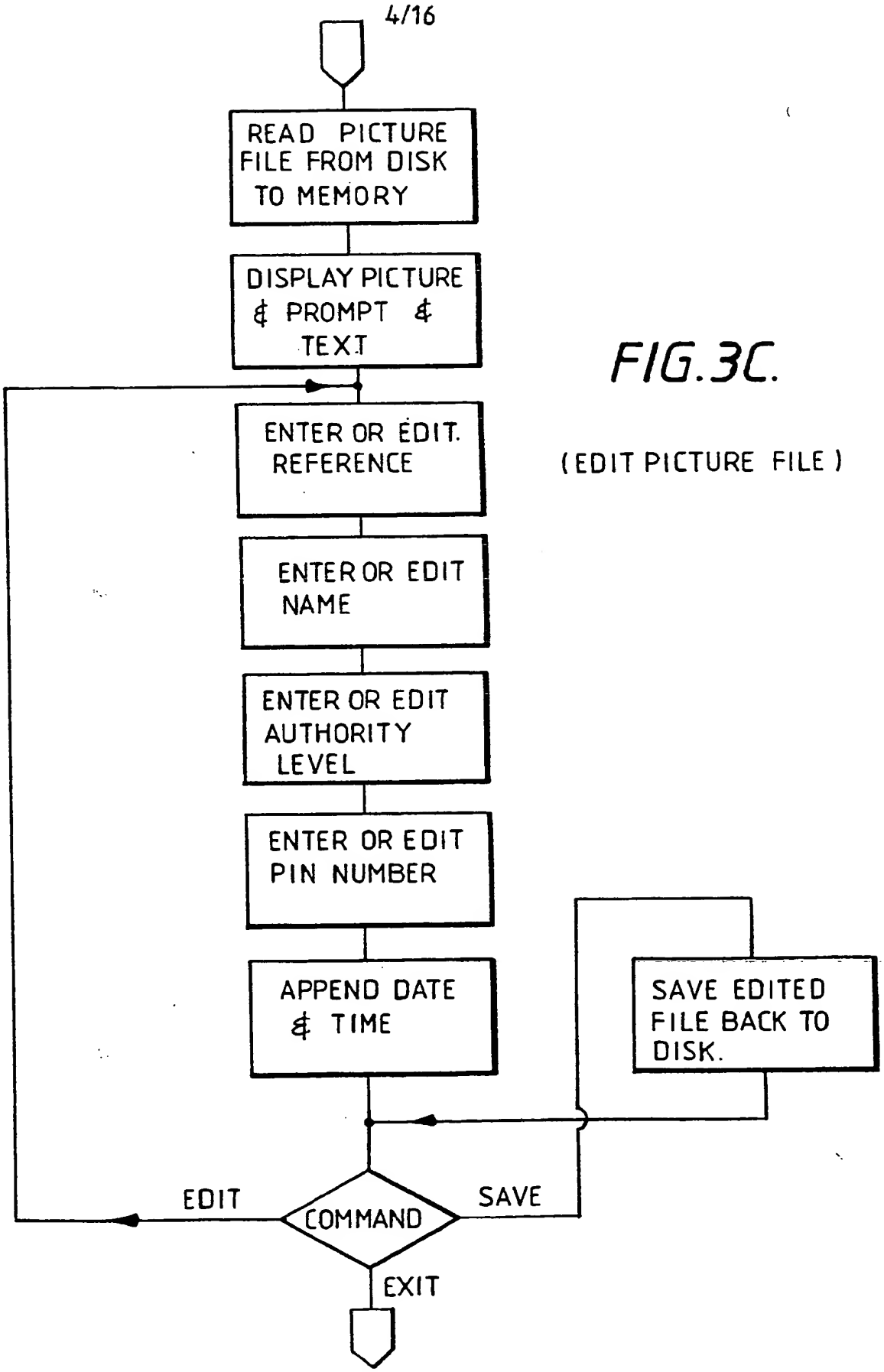


FIG.3C.

(EDIT PICTURE FILE)

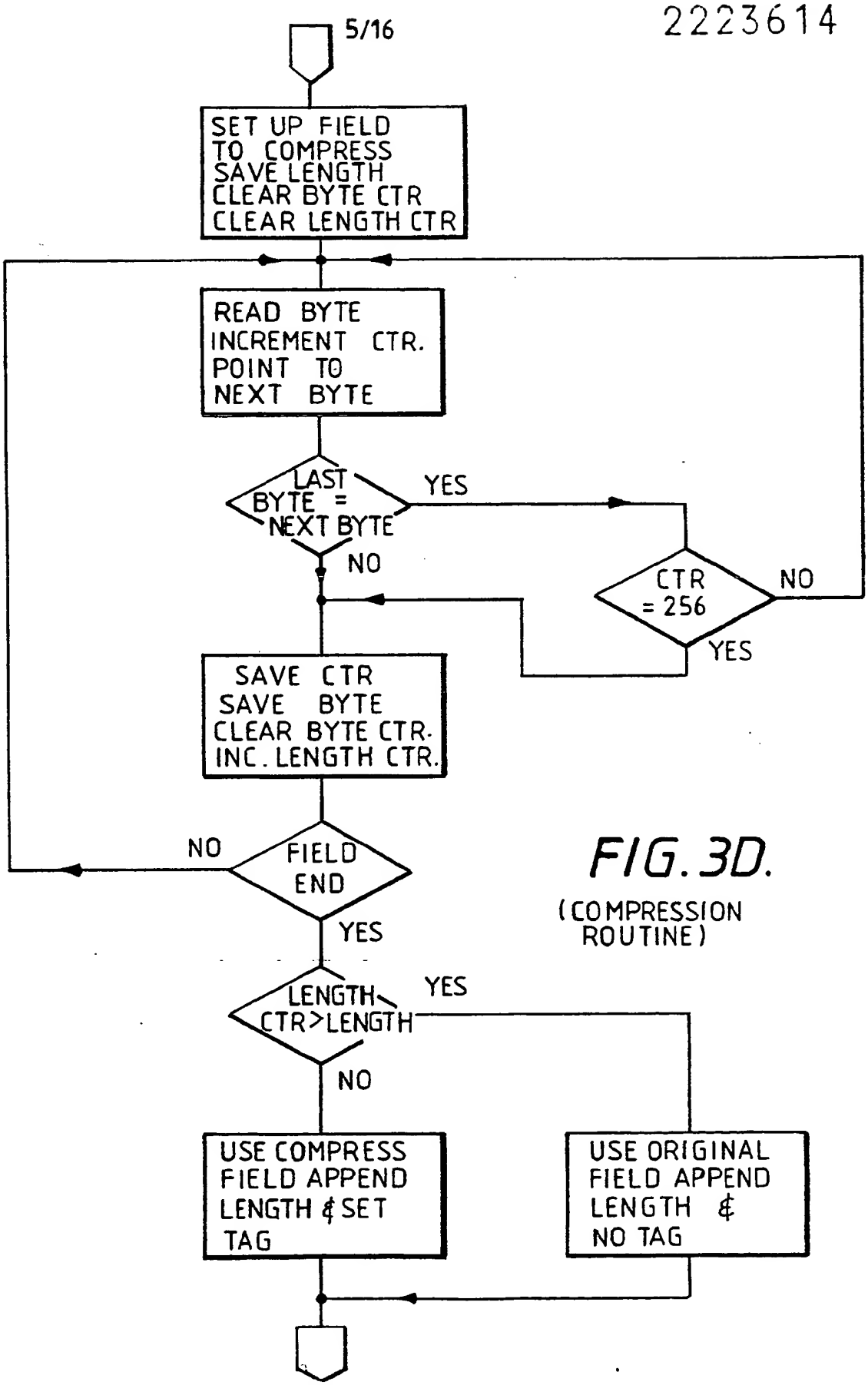


FIG. 3D.

(COMPRESSION ROUTINE)

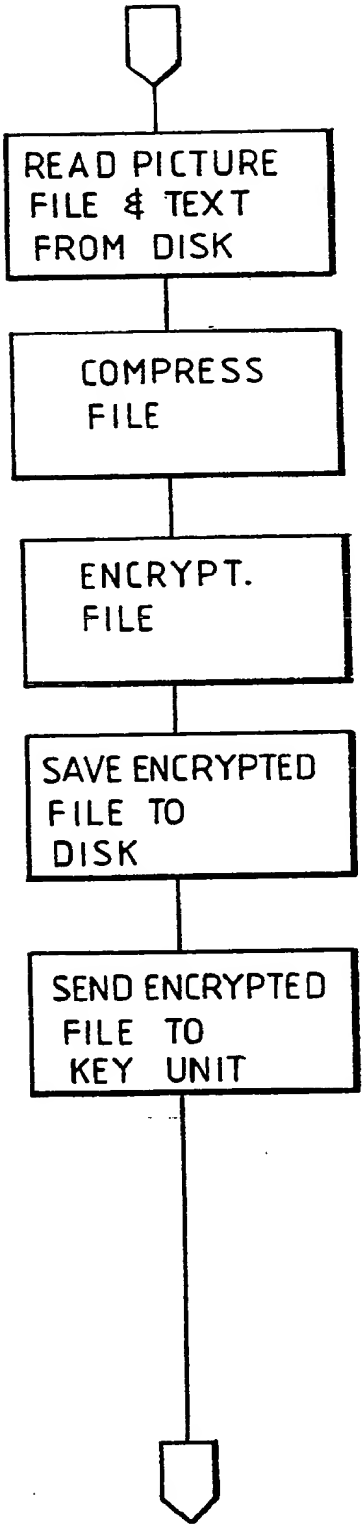


FIG. 3E.

LOAD PICTURE TO KEY

FIG.4.

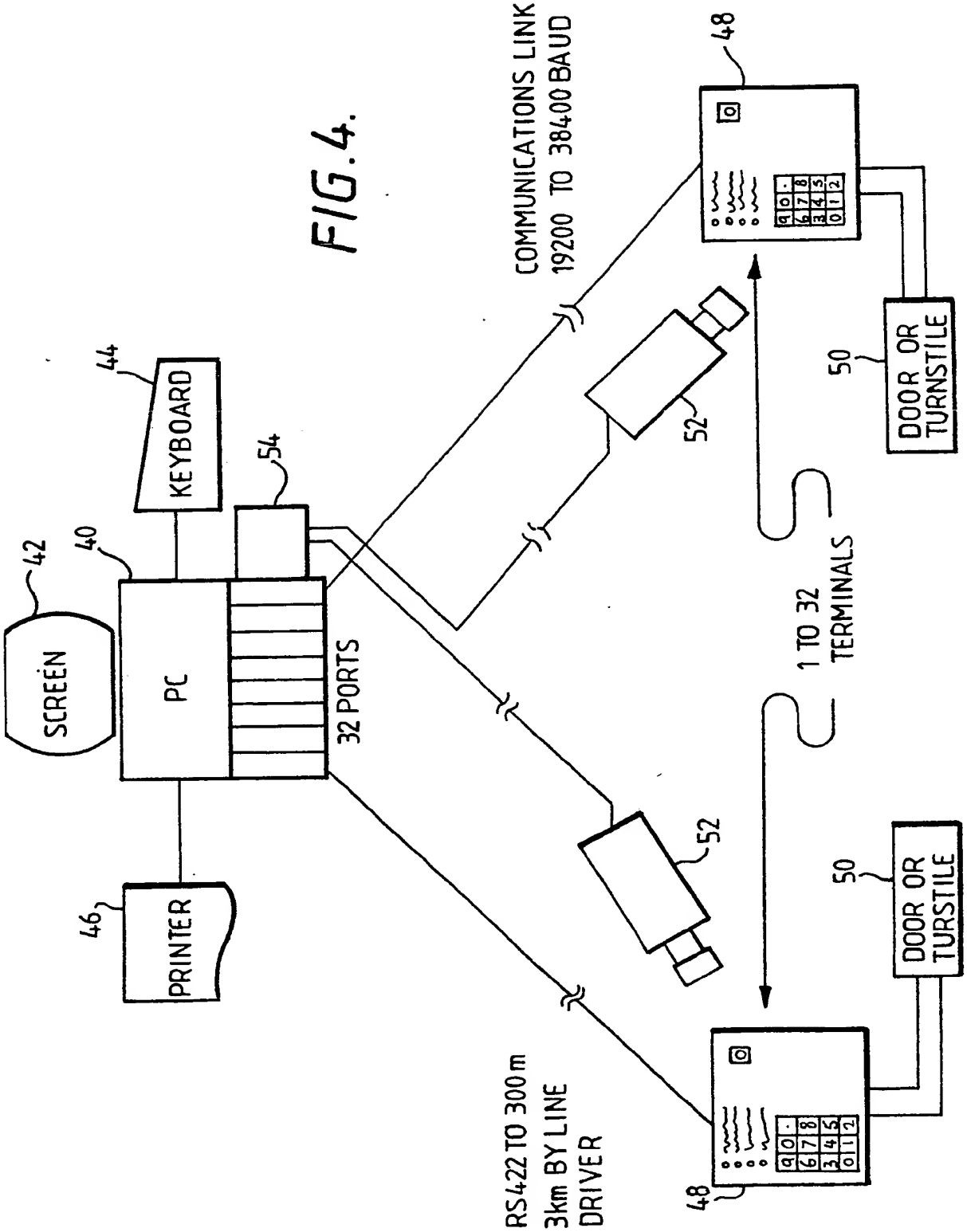
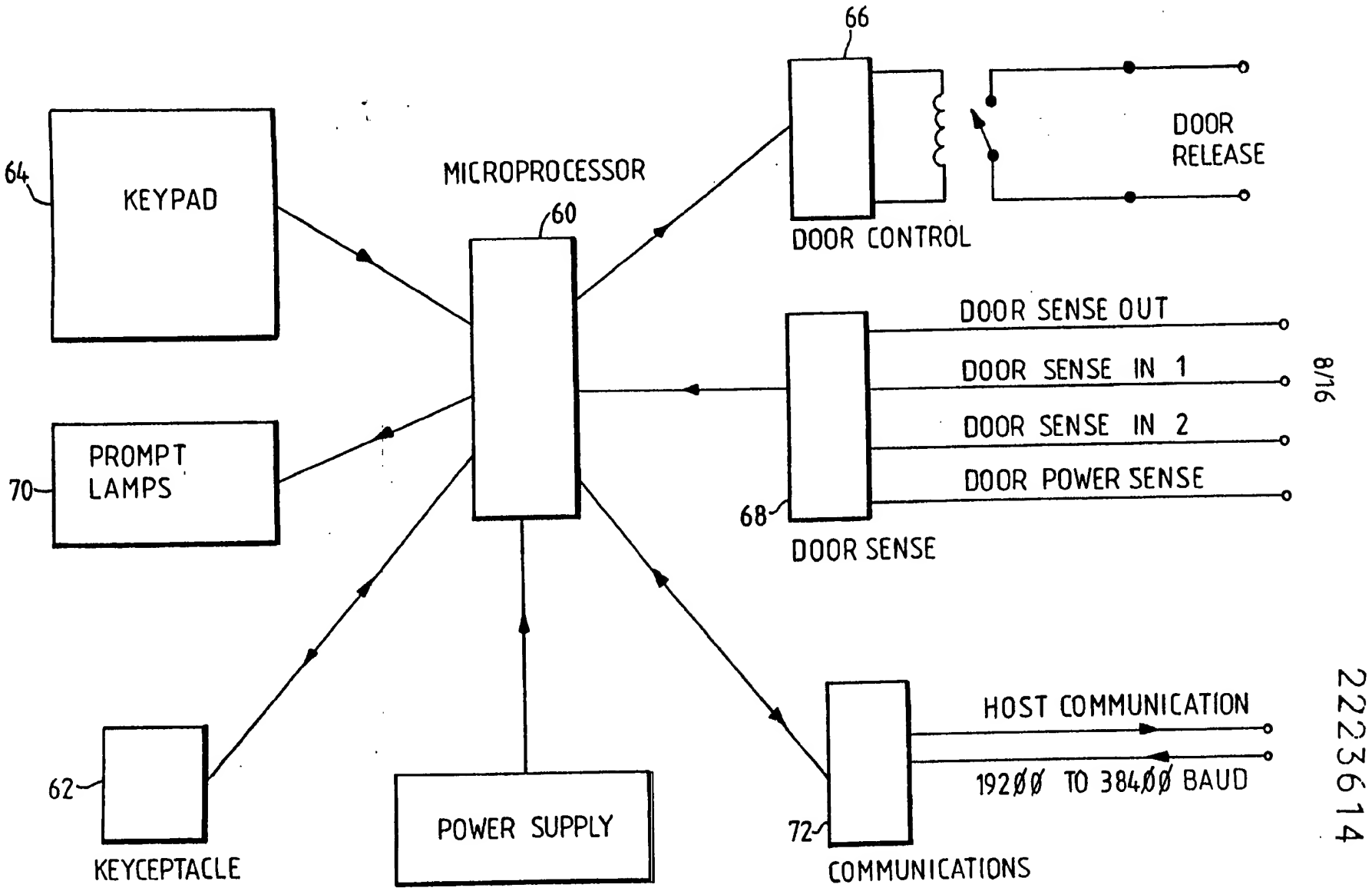

COMMUNICATIONS LINK
19200 TO 38400 BAUD
RS422 TO 300m
3km BY LINE
DRIVER
1 TO 32
TERMINALS
32 PORTS
SCREEN
PC
KEYBOARD
PRINTER
DOOR OR
TURNSTILE
42
40
44
46
48
50
52
54

FIG.5.



8/16

2223614

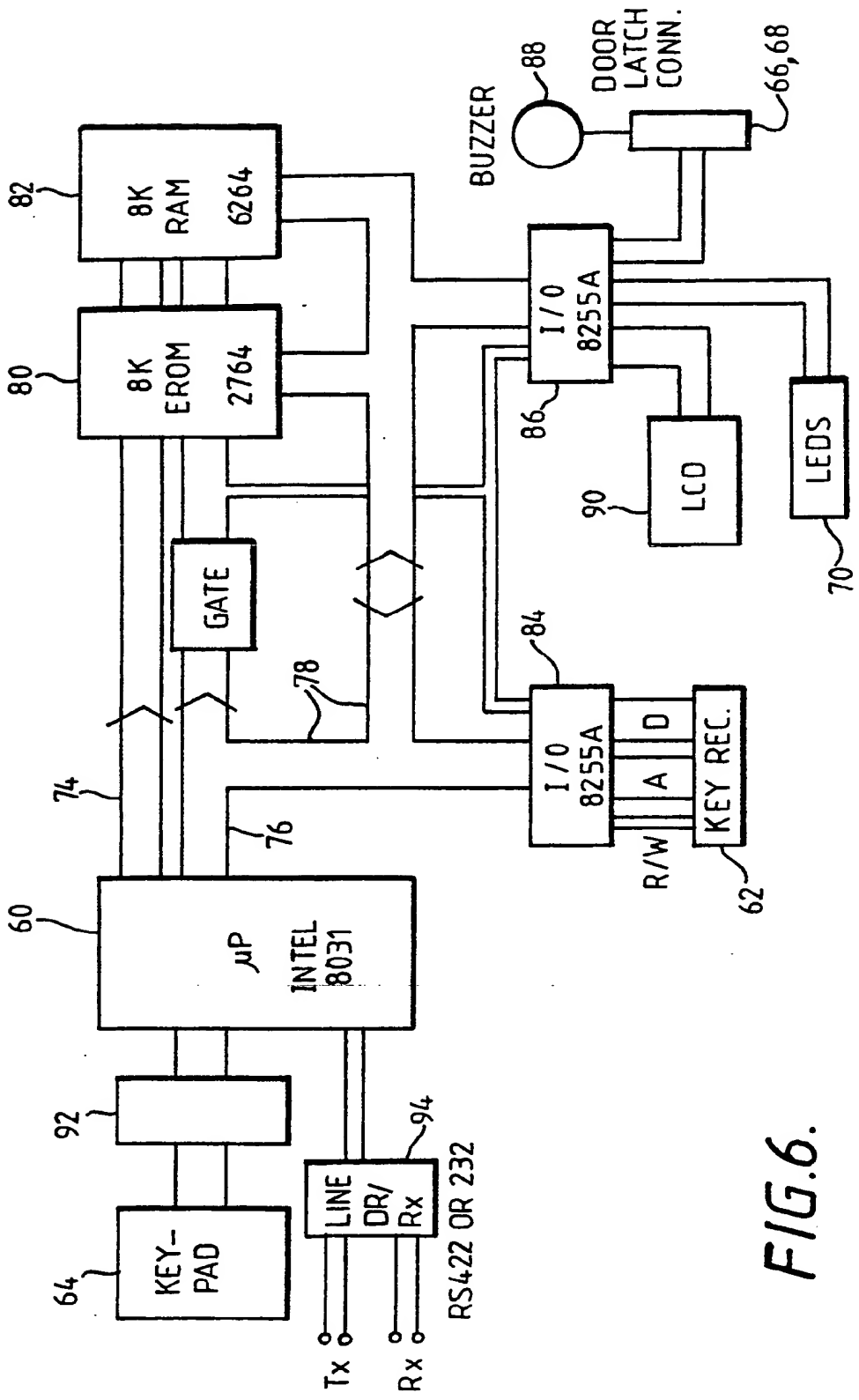

8K RAM 6264
82
8K EROM 2764
80
BUZZER
88
DOOR LATCH CONN.
66,68
I/O 8255A
86
LCD
90
LEDS
70
GATE
78
84
I/O 8255A
D
A
KEY REC.
R/W
62
74
76
60
µP INTEL 8031
92
LINE DR/ Rx
94
KEY-PAD
64
RS422 OR 232
Tx
Rx

FIG.6.

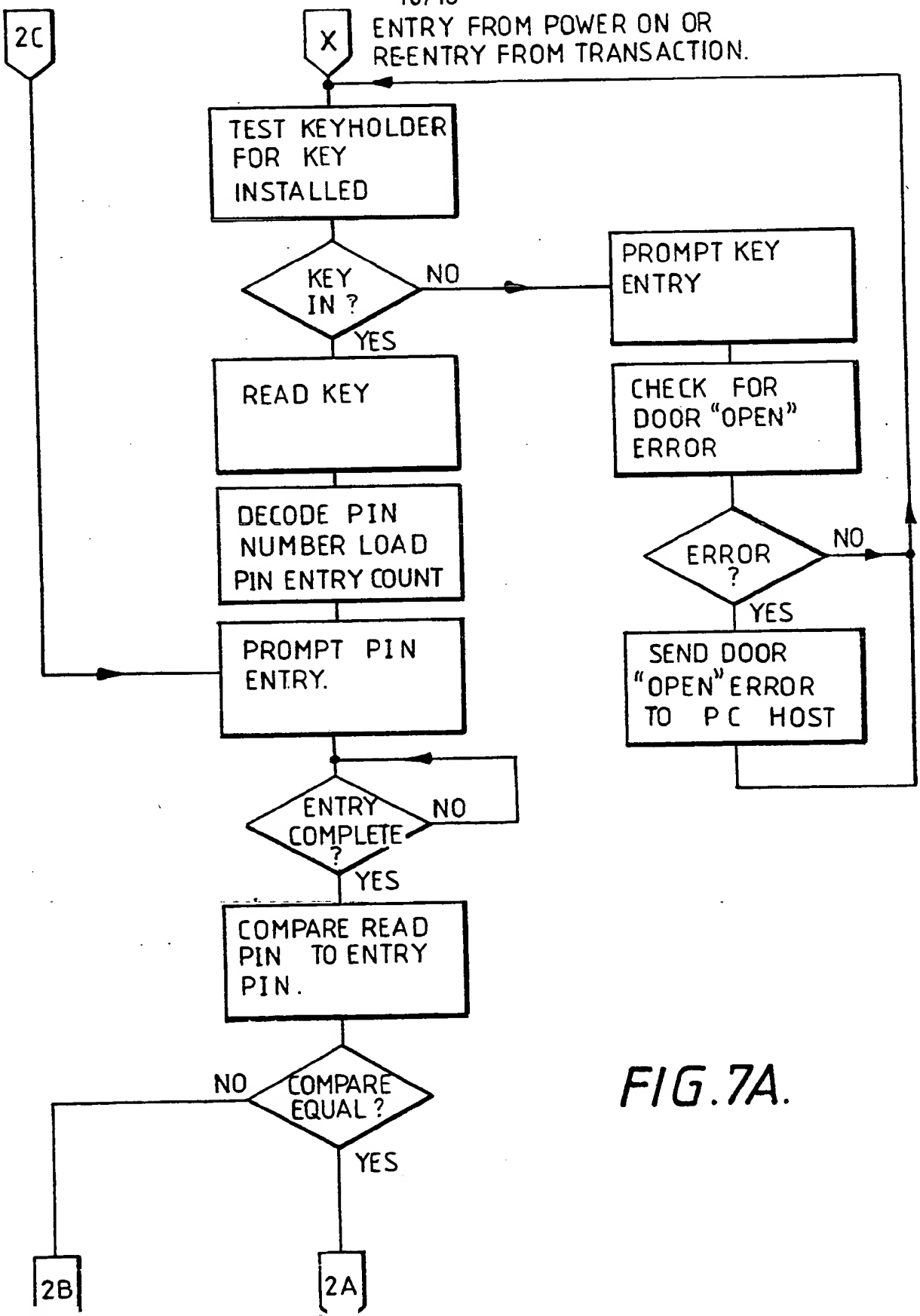

2C
X
ENTRY FROM POWER ON OR RE-ENTRY FROM TRANSACTION.
TEST KEYHOLDER FOR KEY INSTALLED
KEY IN ?
NO
YES
PROMPT KEY ENTRY
READ KEY
CHECK FOR DOOR "OPEN" ERROR
DECODE PIN NUMBER LOAD PIN ENTRY COUNT
ERROR ?
NO
YES
PROMPT PIN ENTRY.
SEND DOOR "OPEN" ERROR TO PC HOST
ENTRY COMPLETE ?
NO
YES
COMPARE READ PIN TO ENTRY PIN.
NO
COMPARE EQUAL ?
YES
2B
2A

FIG. 7A.

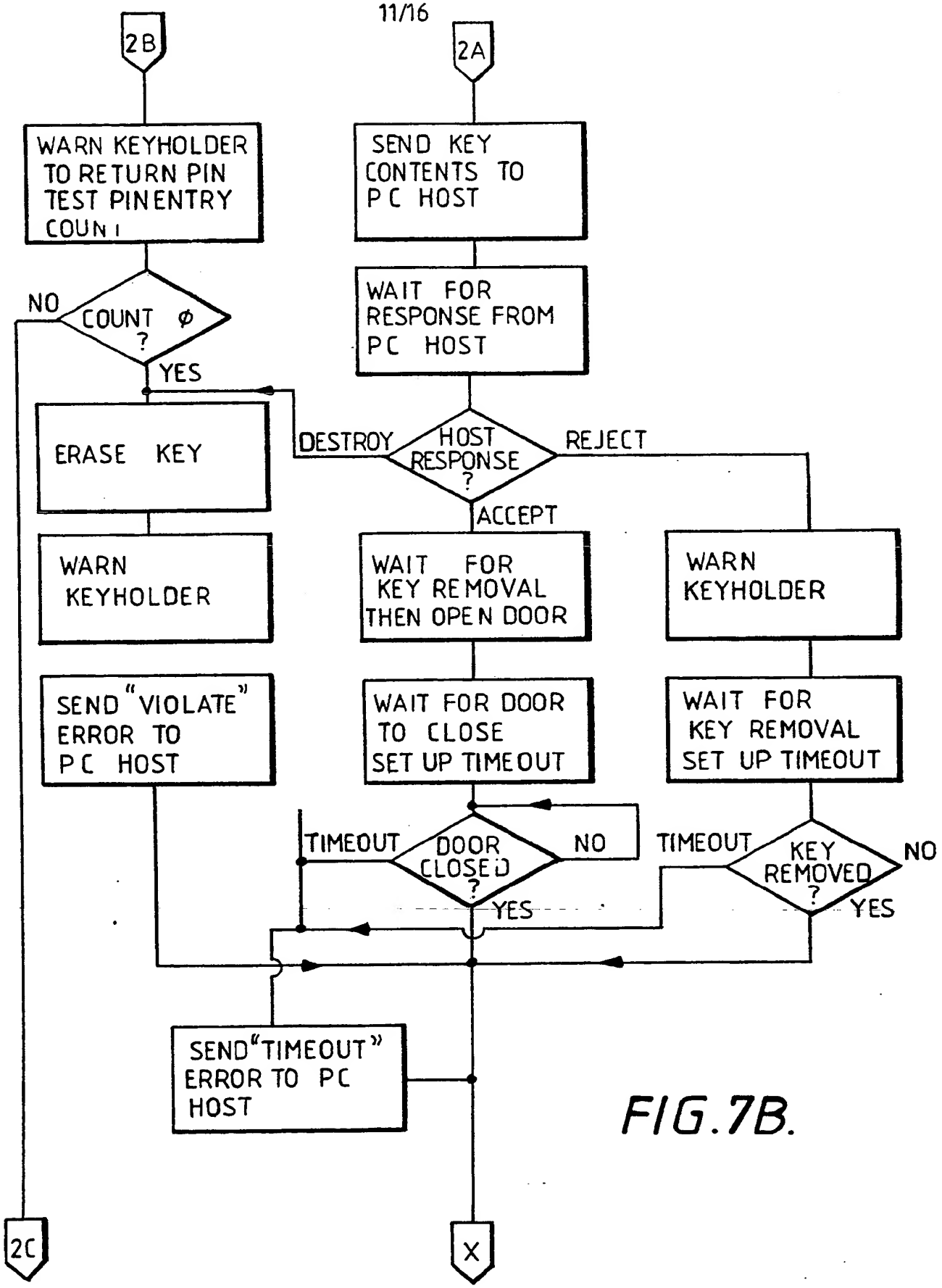

2B
2A
WARN KEYHOLDER TO RETURN PIN TEST PINENTRY COUNT
SEND KEY CONTENTS TO PC HOST
NO
COUNT ϕ ?
WAIT FOR RESPONSE FROM PC HOST
YES
ERASE KEY
DESTROY
HOST RESPONSE ?
REJECT
ACCEPT
WARN KEYHOLDER
WAIT FOR KEY REMOVAL THEN OPEN DOOR
WARN KEYHOLDER
SEND "VIOLATE" ERROR TO PC HOST
WAIT FOR DOOR TO CLOSE SET UP TIMEOUT
WAIT FOR KEY REMOVAL SET UP TIMEOUT
TIMEOUT
DOOR CLOSED ?
NO
YES
TIMEOUT
KEY REMOVED ?
NO
YES
SEND "TIMEOUT" ERROR TO PC HOST
2C
X

FIG.7B.

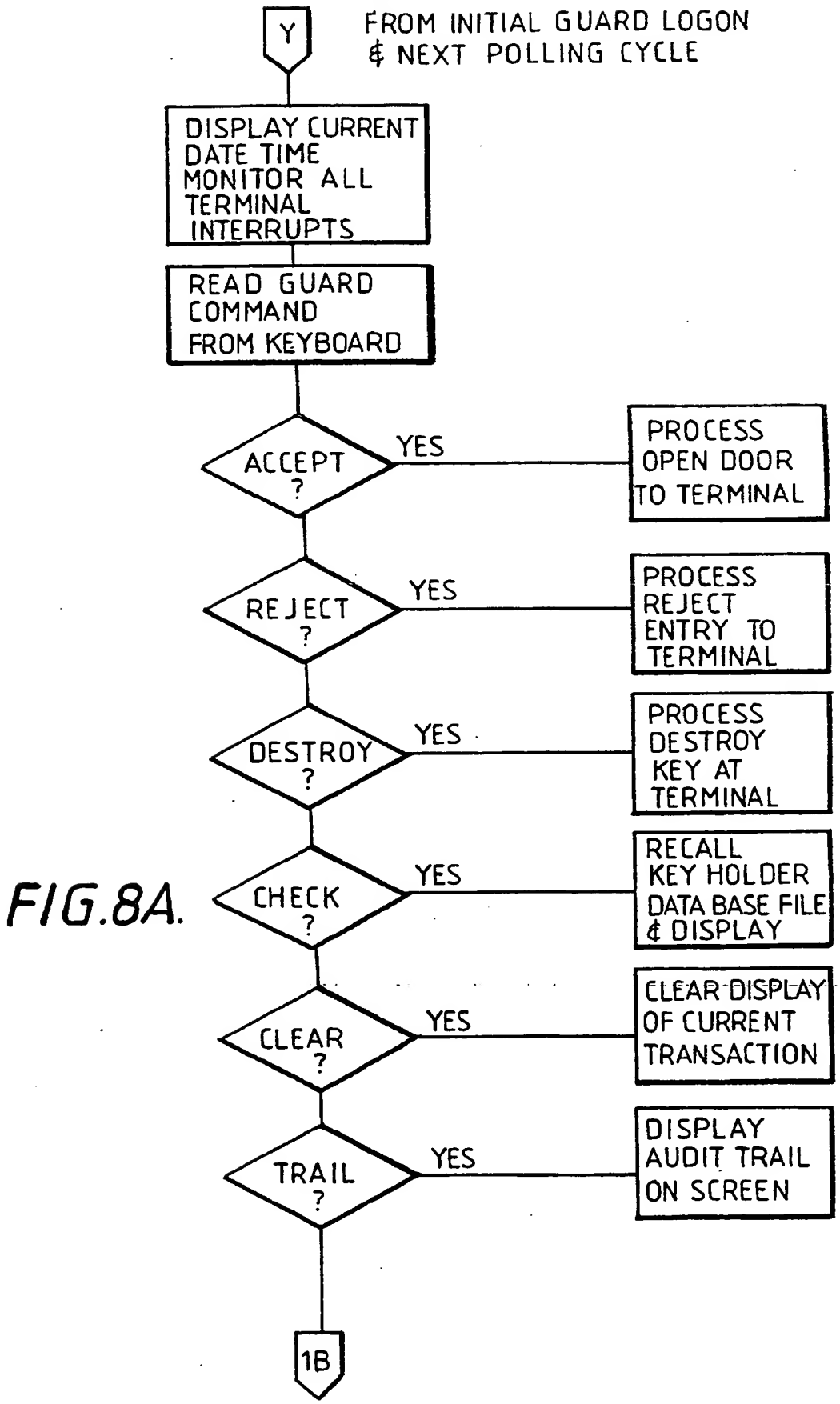

Y
FROM INITIAL GUARD LOGON
& NEXT POLLING CYCLE
DISPLAY CURRENT DATE TIME MONITOR ALL TERMINAL INTERRUPTS
READ GUARD COMMAND FROM KEYBOARD
ACCEPT ?
YES
PROCESS OPEN DOOR TO TERMINAL
REJECT ?
YES
PROCESS REJECT ENTRY TO TERMINAL
DESTROY ?
YES
PROCESS DESTROY KEY AT TERMINAL
CHECK ?
YES
RECALL KEY HOLDER DATA BASE FILE & DISPLAY
CLEAR ?
YES
CLEAR DISPLAY OF CURRENT TRANSACTION
TRAIL ?
YES
DISPLAY AUDIT TRAIL ON SCREEN
1B

FIG.8A.

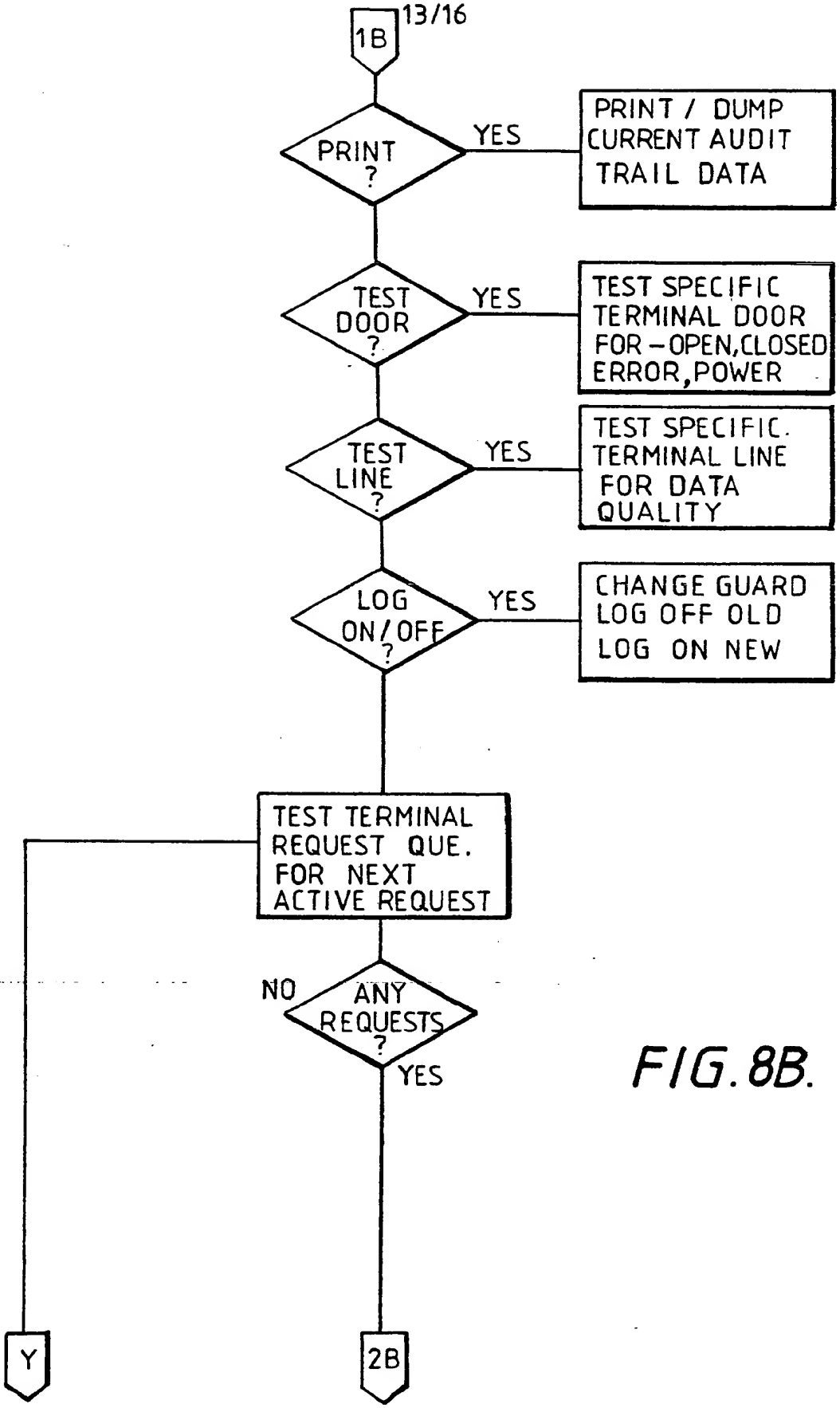

1B
PRINT ?
YES
PRINT / DUMP CURRENT AUDIT TRAIL DATA
TEST DOOR ?
YES
TEST SPECIFIC TERMINAL DOOR FOR – OPEN, CLOSED ERROR, POWER
TEST LINE ?
YES
TEST SPECIFIC. TERMINAL LINE FOR DATA QUALITY
LOG ON/OFF ?
YES
CHANGE GUARD LOG OFF OLD LOG ON NEW
TEST TERMINAL REQUEST QUE. FOR NEXT ACTIVE REQUEST
NO
ANY REQUESTS ?
YES
Y
2B

FIG. 8B.

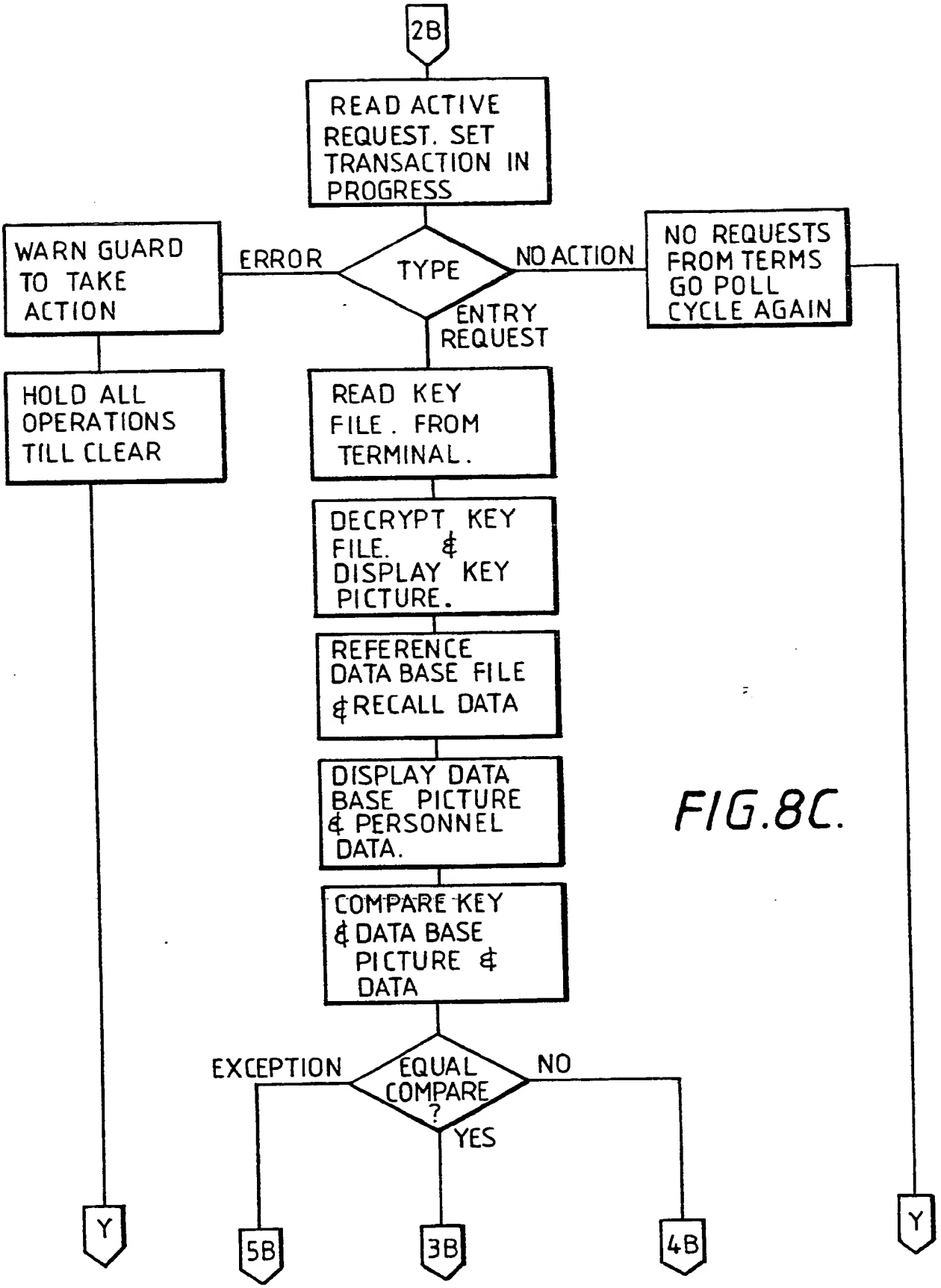

2B
READ ACTIVE REQUEST. SET TRANSACTION IN PROGRESS
TYPE
ERROR
NO ACTION
ENTRY REQUEST
WARN GUARD TO TAKE ACTION
NO REQUESTS FROM TERMS GO POLL CYCLE AGAIN
HOLD ALL OPERATIONS TILL CLEAR
READ KEY FILE. FROM TERMINAL.
DECRYPT KEY FILE. & DISPLAY KEY PICTURE.
REFERENCE DATA BASE FILE & RECALL DATA
DISPLAY DATA BASE PICTURE & PERSONNEL DATA.
COMPARE KEY & DATA BASE PICTURE & DATA
EXCEPTION
EQUAL COMPARE ?
NO
YES
Y
5B
3B
4B
Y

FIG.8C.

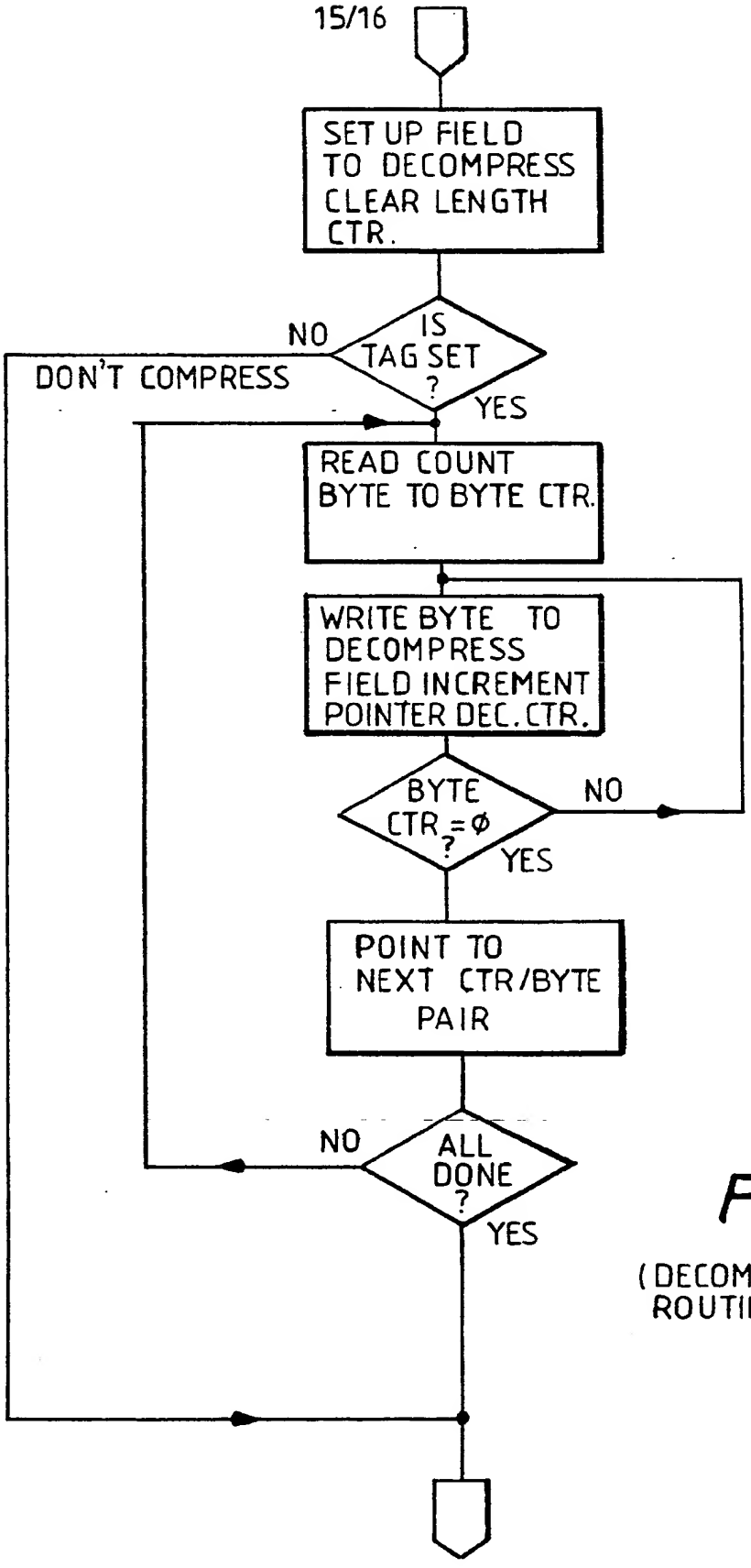


FIG.8D.

(DECOMPRESSION ROUTINE)

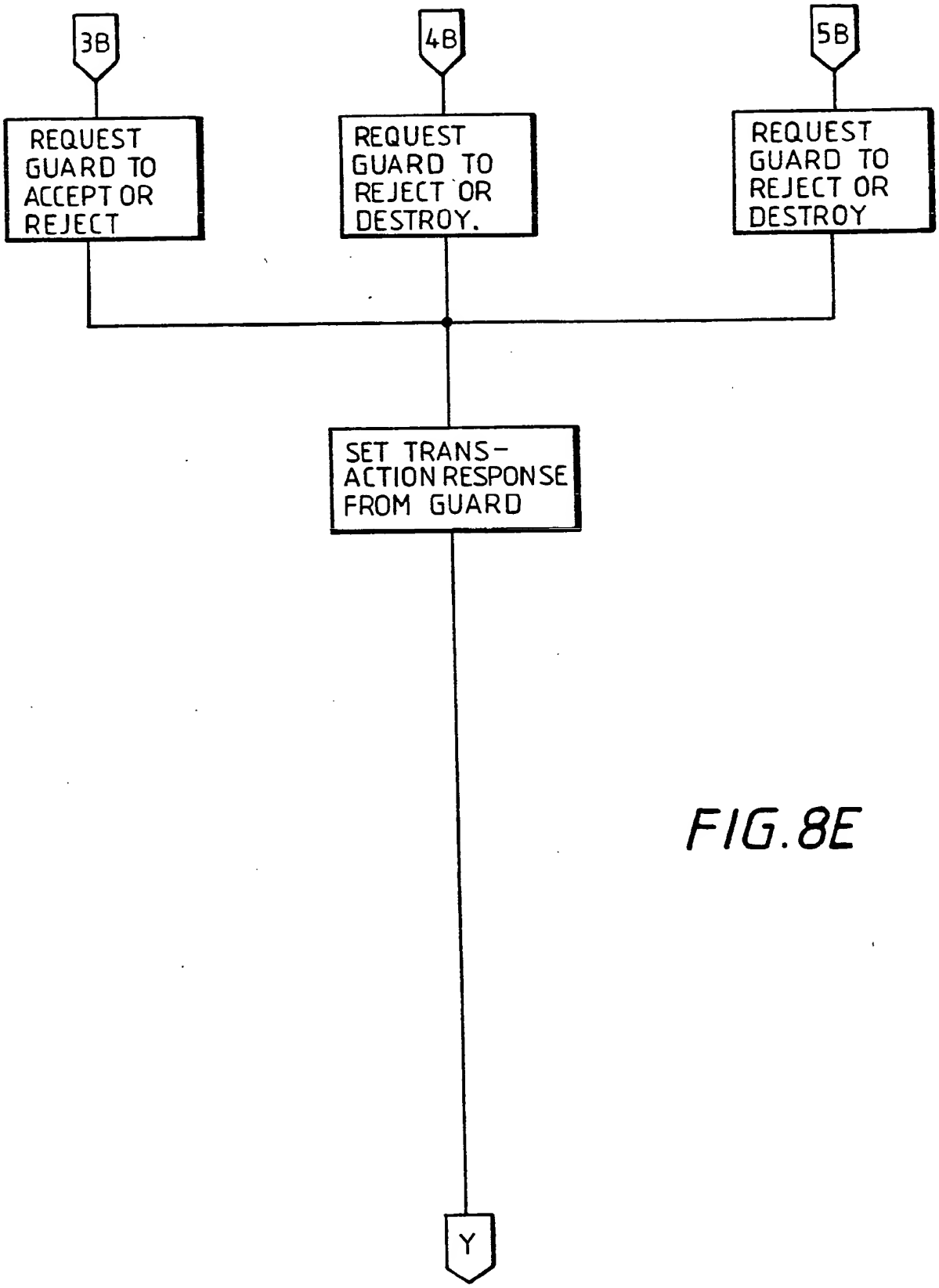

3B
4B
5B
REQUEST GUARD TO ACCEPT OR REJECT
REQUEST GUARD TO REJECT OR DESTROY.
REQUEST GUARD TO REJECT OR DESTROY
SET TRANS-ACTION RESPONSE FROM GUARD
Y

FIG.8E

SECURITY DEVICE AND SYSTEM

This invention relates to a security device for identification of a person, to a security system including the device, to a method of making the device, and to a method of using the system. The device and system have particular use in restricting access to a sensitive area and in financial transactions.

In a world where armed crime, terrorism, political and industrial espionage and fraud are commonplace, there is an increasing need to protect secure areas from unwanted intrusion. A multiplicity of systems for identifying a person for the purpose of either allowing or preventing access have been developed. These include various devices carried by the person to be identified, such as a printed pass bearing a photograph of the user for display to a guard, a magnetic swipe card bearing a name and possibly a number, together with a personal identification number (PIN) for comparison with a number entered by the user on a keypad when seeking access, and a memory key with a non-volatile read-only memory (ROM) containing the same kind of information as the swipe card. All of these are low cost devices but have the disadvantage of being relatively easy to forge or override. The Weigand card is more secure, having a wire with data written on it, but it is more expensive to make and writing of data to the wire is slower than with the devices referred to above.

It is an object of this invention to provide a low cost device offering greater security than those referred to above yet which is convenient in use.

According to a first aspect of this invention a security device for identifying the user of the device comprises data storage means containing picture data representative of a picture of the user. When connected to a suitable display unit operated by security personnel, the picture may be display but, unlike a

simple printed card with a photograph, the picture is not available to the user and is thus difficult to forge. In effect, the device, when coupled to the unit, provides visual identification by comparison of the stored picture with the face of the user by, for example, a guard controlling access to a sensitive area or by retailing staff when handling a credit based transaction.

In addition to providing the security of a hidden picture, the device may include other data such as a PIN number which the user must enter by punching it out on a keypad to obtain access or as part of the identification process, thereby providing an automatic second level of verification using a single portable security device.

The device may take the form of a key containing a non-volatile read-only memory, preferably an electrically erasable programmable read-only memory (EEPROM) with metal contacts along edges of the key for connection to the corresponding contacts of a key reader. Alternatively, a similar kind of memory may be contained in a card with a microprocessor for communicating with a card reader, a so-called "smart" card. The capacity of the memory is preferably less than or equal to 256 kilobits, and typically is in the region of 64 kilobits.

The information contained in the device, including the picture data, can be made more difficult to forge by encryption of the stored data, a step which can also be used to increase security of information transmitted from the key.

The picture data is also preferably in the form of processed video data, the purpose of the processing being to reduce the memory space requirement. In particular the data is based on a reduced grey scale level and may also include data words each representative of several pixels when adjacent pixels all have the same brightness.

According to another aspect of the invention, a security system comprises a data processing unit having means for storing information relating to a plurality of persons for identification purposes, at least one identification terminal coupled to the data processing unit, and a plurality of portable security devices, the terminal including means for reading the security devices carried by the said persons for identification purposes, wherein the terminal is arranged to receive signals representing picture data from the security devices and to transmit corresponding signals to the data processing unit.

The system, in its preferred form, includes a television camera located at or adjacent each identification terminal and coupled to transmit video pictures of persons at the identification terminal to the data processing unit, the data processing station further comprising a display allowing visual comparison of pictures transmitted from the camera with pictures derived from the picture data received from the security devices. A memory associated with the data processing unit may be provided for storing reference picture data representing pictures of persons holding said security devices, the data processing unit further being arranged to display corresponding reference pictures simultaneously with pictures corresponding to data received from security devices presented at the or each identification terminal for visual comparison. Preferably, the reference picture data and the data stored by the security devices have common origins and the data processing unit is arranged automatically to compare the respective data as an automatic identification check.

To improve security against misuse of the system when one or more of the said identification terminals are spaced from the data processing station, the data contained in signals transmitted from the or each

terminal to the data processing unit are in encrypted form, the processing unit being arranged to decrypt the data, preferably in real time.

In operation of the system, the security device of a user is presented to an identification terminal and picture data stored in the device is read from the device and transmitted to the data processing unit which includes a display. A picture derived from the picture data by the processing unit appears on the display where it may be compared by an operator with the user standing by the terminal. In the case of the operator being at a different place from the terminal, a television system including a camera in or adjacent the terminal provides a real time image of the user for the comparison. If the picture obtained from the data stored in the security device matches the face of the user, the user may be allowed, for example, to enter a restricted area through a door or turnstile, or to complete a financial transaction.

The operation of the system may also include the user entering a PIN number at the terminal which is compared with data received from the security device or with centrally stored data, before the user's identity is considered to have been verified. In addition, reference picture data corresponding to that in the security device may be stored in a meomory associaed with the data processing unit for comparison with the received picture data as a further identity check.

The invention also provides a method of producing the security device carried by a user. In this method, an image of the user's face obtained, for example, from a TV camera or a photograph, is converted into digital form, the resulting so-called 'raw' picture data is then processed to reduce the total amount of data and the processed data is written to non-volatile storage means in a portable form. Typically the storage means is an

erasable programmable read-only memory contained in a key-shaped package (hereinafter referred to as a key), or a card-like package.

Preferably, the processing of the picture data includes reducing the grey-scale level, i.e. employing a level of brightness quantisation which is coarser than in the raw picture data. Further data content reduction can be achieved by reducing resolution of the image, for example, by averaging a group of adjacent pixels to form a single pixel, and by using the data representing the brightness of one pixel as a reference for a plurality of other pixels, particularly pixels of equal brightness Thus, in scanning the picture data, the data representing a succession of pixels of equal brightness may be converted to a single brightness value and length or number value corresponding to number of subsequent pixels in a line.

The production of the device may involve encryption of the picture data, preferably the processed picture data, prior to writing data to the storage means.

The invention will now be described by way of example with reference to the drawings in which:-

Figure 1 is a diagrammatic view of a portable security key in accordance with the invention:

Figure 2 is a block diagram of a key generation system for producing a security key with stored picture data;

Figures 3A to 3E are flow charts of operations performed by the key generation system under software control;

Figure 4 is a block diagram of part of a security system in accordance with the invention;

Figure 5 is a simplified block diagram of one of the identification or key terminals of the system of Figure 4;

Figure 6 is a more detailed block diagram of part

of the key terminal of Figure 5;

Figures 7A and 7B are flow charts illustrating the operation of the key terminal; and

Figures 8A to 8E are flow charts illustrating the operation of a data processing unit forming a host control station for the security system of Figure 4.

Referring to Figure 1, a preferred security device in accordance with the invention is in the form of a key having, mounted inside a plastic key casing 10, an integrated memory circuit 12 which is a 64 kilobit (8192 x 8) electrically erasable programmable read-only memory (EEPROM). The memory has data and address lines coupled to a plurality of metal contacts 14 mounted along an edge of the key so that when the key is inserted in an appropriate key receptacle with correspondingly positioned slider contacts, the memory can be coupled to circuitry for writing data to or reading data from the memory. A suitable device forming the basis of the key is the model PK 64KS key available from Datakey, Inc., of Burnsville, MN 55337, U.S.A.

In accordance with the invention, the key memory 12 stores picture data representative of a picture of a person whose identity it is to be used to verify. The person may need to be identified in order to verify his or her creditworthiness, or as an authorised user of, for example, certain equipment, or as someone who is authorised to obtain access to a restricted area. For the purposes of the present description, a security system for allowing or preventing access to a restricted area through a door will be considered.

Generation of data and its storage in the key is performed as follows. Referring to Figure 2, a key generation system for this purpose preferably comprises a closed circuit TV camera 20 for producing an image 22 of the user which is digitised in a digitiser 24 by defining the image as a series of points (pixels) of a particular brightness, each pixel being coded as a data

word the value of which represents the brightness. The digitiser 23 is coupled to a personal computer 26, having a keyboard 28 and a screen 30, for manipulating the picture data produced by the digitiser 24, and for feeding the manipulated data to a key write terminal 32 where it is written to the memory in a key such as that described above with reference to Figure 1.

Manipulation of the picture data by the computer 26 is carried according to the flow charts of Figures 3A to 3E. The capture of 'raw' picture data is shown in Figure 3A, it being understood that the data is regarded as being scanned vertically so that the program represented by Figure 3A treats the data in a series of columns, 255 pixels of each column being saved in the computer RAM. When a complete picture has been saved, alternate line bytes are added and the sum divided by two to even the image prior to writing the data to disk.

Next, the picture is processed as shown in Figure 3B by first reducing the image size from 512 x 512 pixels to one of 128 x 128 pixels. This is performed by twice forming a single average value pixel from groups of four pixels (each group being a square 2 x 2 pixels in size). This represents the first step in reducing the memory capacity required to store the image. To correct the scanning orientation the image is then digitally rotated by 90°, after which a further data reduction step is performed by reducing the grey-scale level from the 256 level quantisation of the raw data to a level such as 16, although 8, 32 or 64 level quantisation can be used, depending on the capacity of the key memory and the resolution required.

At this point the image may be displayed on the computer screen if desired, as indicated by the last step in Figure 3B.

In the preferred embodiment of the invention the key contains, in addition to picture data, other data

such as a reference number, the user's name, an authority level, a PIN number, and the data and time when the key data was created and stored. Such data is added to the picture data stored on the computer disk as shown in Figure 3C.

A further reduction in the amount of data needed to store the image can be obtained by the compression routine of Figure 3D. This routine begins with reading from disk the picture data resulting from the steps of Figure 3B, and then looking for successions of bytes having the same brightness value. An identified series of pixels of equal brightness are be expressed in terms of the signal brightness value of all of the bytes and a length value indicating the number of bytes in the series. This routine then tests the total number of bytes against the original number of bytes and if a saving has been made, the "compressed" bytes are used and a corresponding 'tag' is set.

Referring to Figure 3E, the compression routine is followed by encryption of all of the data, writing of the encrypted data to disk and then at a suitable time, the encrypted data is written to the key via the key write terminal (32 in Figure 2). Encryption maintains anonymity of the user except to the operators of a security system in which it is used.

The key, containing processed picture and other data, is usable with a pluarity of other such keys, in a security system incorporating a central data processing unit, hereinafter referred to as the 'host computer', as shown in Figure 4.

The host computer is preferably a personal computer 40 having a screen 42 and a keyboard 44, and has an associated printer 46. The computer 40 is provided with 32 input/output ports for communication with up to 32 key terminals 48 at remote locations, in this example the locations where access to a restricted area can be

gained via a door or turnstile 50. At those locations closed circuit TV cameras 52 are provided and are coupled to a device 54 associated with the computer 40 for allowing the faces of persons at the key terminals 48 to be displayed on the computer screen 42 alongside picture data received from the key terminals. The communications links 56 between the key terminals 48 and the host computer 40 allow passage of signals in both directions.

It will be appreciated that the host computer can act as the computer for generating the key, in conjunction with a scanning video camera and the key generation software.

An outline of the key terminal construction is shown in Figure 5. Each key terminal has its own controlling microprocessor 60. To this microprocessor 60 are coupled a key receptacle 62 for collecting data from inserted keys and, if necessary, for use in erasing the contents of a key, and a keypad 64 for entry of PIN numbers by persons seeking access. Also coupled to the microprocessor 60 are a door latch control circuit 66 for releasing the door, a door sensing circuit 68 for sensing the door position, prompt lamps 70 for indicating to the person seeking access the actions to be performed, and communications circuitry 72 for feeding signals to and receiving signals from the host computer.

Parts of the key terminal are shown in more detail in Figure 6. Referring to Figure 6, the microprocessor 60 has address lines 74, combined address and data lines 76, and a data bus 78. The combined address and data lines 76 are used as address lines when writing to or reading from memories associated with the microprocesser. These memories comprise a ROM 80 for storing a key terminal control program, and a RAM 82 for storage of data from keys prior to transmission of the

data to the host computer. Other uses include the decryption or decoding of PIN numbers.

In addition to being connected to the memories 80, 82, the data bus feeds data between the microprocessor 60 on the one hand and input/output ports 84, 86 on the other hand, which are coupled respectively to the key receptacle 62 for reading from or erasing the key memory, and to the prompt lamps (L.E.D.'s) 70. Door release and sensing circuitry 66, 68 and a buzzer 88 which sounds when the door is released, are also controlled via the second of the input/output devices 86. Provision is made additionally for the operation of a liquid crystal display 90 via the second input/output device 86.

The keypad 64 shown in Figure 5 appears also in Figure 6, shown connected via a buffer device 92 to one of the microprocessor ports. Another port serves for serial transmission of data to and from the host computer via line drives and receivers 94.

Operation of the key terminal is governed by the program stored in the ROM 80 as shown in Figures 7A and 7B. The flow charts of Figures 7A and 7B are largely self-explanatory and are not described in detail here. Briefly, the microprocessor 60 (Figures 5 and 6) is controlled so as to check the position of the door at appropriate times to read and decode the PIN number stored in an inserted key and to compare it with the PIN number entered on the keypad. It causes prompts to be displayed to the user either via the prompt lamps or the liquid crystal display, it causes the contents of the key, including the picture data, to be transmitted to the host computer, and it accepts and carries out commands received from the host computer such as the opening of the door, the rejection of the key, or the destruction of the key contents.

If the user enters an incorrect PIN number the

terminal will keep rejecting it until a predetermined count is reached and the key is automatically erased.

The host computer 40 (Figure 4) is capable of many operations, these being shown in the flow charts of Figures 8A to 8E. Initially, the program of the host computer is designed so as to respond to any of ten commands provided by the operator. For instance, if a person is seeking access at one of the key terminals and the operator is satisfied that the person is authorised to enter, the 'Accept' command is given and signals for causing the door adjacent the terminal to be opened are sent to the terminal. The operator can alternatively cause the key to be rejected or erased by giving 'Reject' or 'Destroy' commands. The computer will have stored in a database details of authorised persons including picture data corresponding to the picture data stored on their keys. This data can be called up on the screen by the 'Check' command. The 'Clear' command clears the display for the next transaction, while the 'Trail' command brings an audit trail onto the screen. Referring now to Figure 8B, this audit trail may be printed or dumped by giving the 'Print' command. Any selected door may be tested using the 'Test Door' command and subsequent commands (not shown). Similarly a 'Test Line' command can be used for testing selected lines between the host computer and the key terminals. Finally, there is a standard Log on/Log off command.

Having polled for the presence of these ten commands, this program then tests a 'terminal request' queue for the next active request, which is normally an indication that a person is seeking access.

Referring to Figure 8C, an entry request in which the PIN number comparison carried out by the terminal indicates a PIN number match causes the key file of the key terminal to be read to the host computer. The

received key data is decrypted in real time by the host computer and displayed. The display includes the processed picture data stored in the key inserted in the key receptacle at the terminal. If the compression tag is 'set', a decompression routine, shown in Figure 8D is performed prior to display.

The computer is programmed automatically on receipt of the key file to retrieve the corresponding data from its database file and to compare the received picture and other data with that from the database file. A match produces an 'Accept' or 'Reject' message for the operator, as shown in Figure 8E, whereupon the operator would compare the picture data with the picture received from the camera at the key terminal. If satisified that the person is authorised to enter, the operator gives the 'Accept' command referred to above.

If, on the other hand, the automatic checks do not produce a match, the operator is given the option of rejection or erasure of the key. The person at the key terminal may be informed via an audio link between the host computer and the terminal to go a manned security station for checking or issue of a new key. Preferably each key terminal has both a loudspeaker and a microphone to allow 2-way voice communication.

The host computer control program shown in Figures 8A to 8E runs in real time with interrupt driven front end communications. The program can only be loaded by an operator with the correct password and will continue to run until the system is deactivated under password control.

CLAIMS

1. A security device for identifying the user of the device, comprising data storage means containing picture data representative of a picture of the user.

2. A device according to claim 1, in the form of a key containing a non-volatile memory, the key having contacts for connection to corresponding contacts of a key reader.

3. A device according to claim 1, in the form of a card having a non-volatile memory.

4. A device according to claim 1 or claim 3, in the form of a card having a microprocessor for communicating with a card reader.

5. A device according to claim 2 or claim 3, wherein the memory has a capacity of less than or equal to 256 kilobits.

6. A device according to any preceding claim, wherein the storage means are operable to store processed video data.

7. A device according to claim 6, wherein the processed video data is based on a reduced grey scale.

8. A security system comprising a data processing unit having means for storing information relating to a plurality of persons for identification purposes, at least one identification terminal coupled to the data processing unit, and a plurality of portable security devices, the terminal including means for reading the security devices carried by the said persons for

identification purposes, and the terminal being arranged to receive signals representing picture data from the security devices and to transmit corresponding signals to the data processing unit.

9. A system according to claim 8, wherein the portable security devices are in the form of keys each containing a non-volatile read-only memory.

10. A system according to claim 8, wherein the portable security device are in the form of cards each having a non-volatile read-only memory.

11. A system according to any of claims 8 to 10, further comprising a television camera located at or adjacent each terminal and coupled to transmit video pictures of persons at the identification terminal to the data processing unit.

12. A system according to claim 11, wherein the data processing unit includes a display arranged to receive pictures transmitted from the camera for allowing visual comparison of the pictures with pictures derived from picture data received from the security devices.

13. A system according to any of claims 8 to 11, wherein the data processing unit includes a memory operable to store reference picture data representing pictures of persons holding the security devices.

14. A system according to claim 13, wherein the data processing unit is arranged to display reference pictures corresponding to the reference picture data simultaneously with pictures corresponding to data received from the security devices presented at the or each identification terminal for visual comparison.

15. A system according to claim 13 or claim 14, wherein the data processing unit is arranged automatically to compare the reference picture data with the data stored by the security devices.

16. A system according to any of claims 8 to 15, wherein the or each terminal is operable to transmit picture data signals in encrypted form, and the data processing unit is arranged to decrypt the data signals in real time.

17. A method of operating a security system, the system being as defined in any of claims 8 to 16, wherein the method comprises presentation of a security device by the user to an identificaton terminal, reading of stored picture data from the security device by the terminal and transmission of the stored picture data to the data processing unit, displaying a picture derived from the picture data on a display forming part of the data processing unit, comparing the displayed picture with the user.

18. A method according to claim 17 for operating a security system according to claim 11, wherein the picture derived from the picture data read from the security device is compared with a television image of the user.

19. A method according to claim 17 to claim 18, further including entry of a PIN number by the user at the terminal, and comparing the entered number with data received from the security device.

20. A method of producing a security device for identifying the user of the device, including converting an image of the user's face into digital picture data,

processing the data to reduce the amount of data, writing the processed data to a non-volatile storage means forming part of the device.

21. A method according to claim 20, wherein the processing of the picture data includes reducing the grey scale level.

22. A method according to claim 20 or claim 21, wherein the processing of the picture data includes reducing the resolution of the image represented by the data.

23. A method according to claim 22, wherein the resolution reduction is performed by averaging a group of adjacent picture data pixels to form a single pixel.

24. A method according to any of claims 20 to 23, wherein the processing of the picture data includes using data representing the brightness of one pixel as a reference for a purality of other pixels.

25. A method according to any of claims 20 to 24, including encrypting the picture data prior to writing it to the storage means.

26. A security device constructed and arranged substantially as herein described with reference to the drawings.

27. A method of producing a security device, the method being substantially as herein described with reference to the drawings.

28. A security system constructed and arranged substantially as herein described with reference to the drawings.

29. A method of operating a security system, the method being substantially as herein described with reference to the drawings.

Published 1990 at The Patent Office, State House, 66 71 High Holborn, London WC1R 4TP Further
Sales Branch, St Mary Cray, Orp